IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW HAMPSHIRE

IN THE MATTER OF THE SEARCH OF A SAMSUNG GALAXY A03, IMEI 357815981123565, PRESENTLY SECURED AT HOMELAND SECURITY INVESTIGATIONS, MANCHESTER, NH	Case No. 24-mj-92-01-TSM

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR SEARCH WARRANT

I, Adam Rayho, a Special Agent with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), being duly sworn, depose and state as follows:

INTRODUCTION

1. In May 2022, in my capacity as a Task Force Officer assigned to HSI, I began an investigation into offenses of distribution and possession of child pornography via the Peer to Peer Network BitTorrent, which had been occurring from a wireless internet address belonging to the Crane Restaurant, located at 113 W Pearl Street, Unit 2, Nashua, NH ("SUBJECT PREMISES"). The target of this investigation was identified as Dwayne Frechette ("FRECHETTE"), a delivery driver for the restaurant. During the execution of a federal search warrant in July 2022 at the SUBJECT PREMISES (22-mj-139-01-AJ) FRECHETTE informed investigators he had purchased multiple cell phones and stated one of them was currently within his vehicle. An additional search warrant (22-mj-144-01-AJ) was granted for FRECHETTE's vehicle and a Samsung Galaxy A03 ("SUBJECT DEVICE") belonging to FRECHETTE was

seized. A subsequent review of the SUBJECT DEVICE only captured a limited extraction as the phone was locked and the password was unknown. As will be shown below, there is probable cause to believe that evidence, fruits, and instrumentalities of distribution and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2), and 2252A(a)(5)(B) are present within the SUBJECT DEVICE. I submit this affidavit in support of a warrant under Rule 41 of the Federal Rules of Criminal Procedure to search the SUBJECT DEVICE, which is further described in Attachement A incorporated herein by reference, for the things described in Attachement B – specifically, evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252A(a)(2), and 2252A(a)(5)(B), which relates to the distribution and possession of child pornography.

2. This affidavit is based in part on information that I learned from discussions with other law enforcement officers and on my own investigation of this matter. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the violation of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B), are presently located within the SUBJECT DEVICE.

AGENT BACKGROUND

3. I am a Special Agent with Homeland Security Investigations ("HSI") assigned to the Boston Field Office and have been employed by HSI since May 2023. My primary responsibility is as a criminal investigator assigned to the Cyber Crimes Group. As a member of the Cyber Crimes Group, I am responsible for conducting investigations involving crimes that have a nexus to the clearnet or dark web. Prior to becoming a Special Agent, I was a detective

with the Nashua, New Hampshire Police Department, and a deputized task force officer (TFO) for HSI. I became a certified police officer in the State of New Hampshire in May 2014 after graduating from the 164th New Hampshire Police Standards and Training Academy. I hold a bachelor's degree in criminal justice, with a minor in computer science and victimology, from Endicott College. I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant.

4. During my career, I have investigated criminal violations related to online sexual exploitation of children. I have received training in the areas of child sexual exploitation including, but not limited to, possession, distribution, receipt, and production of child pornography, and interstate travel with intent to engage in criminal sexual activity, by attending training hosted by the ICAC involving online undercover chat investigations and interview/interrogation. I have participated in numerous online trainings hosted by the Federal Bureau of Investigation Child Exploitation and Human Trafficking Task Force Online Covert Employee Development Series. These trainings focused on live stream investigations and using undercover personas on various social media applications for proactive investigations. I have also attended the National Law Enforcement Conference on Child Exploitation where I took classes on using undercover personas, IRC investigations, and investigations on BitTorrent and the Freenet. I have personally conducted numerous online undercover investigations using social media applications such as KIK messenger, Grindr, WhatsApp, Whisper, and MeetMe along with investigation on Peer to Peer networks. In addition, I have completed the Cellebrite Certified Operator and Cellebrite Certified Physical Analyst course in mobile forensics. Furthermore, I have completed additional trainings offered by the Internet Crimes Against

Children Task Force, National Training Program which is a program of the Fox Valley Technical College – National Criminal Justice Training Center, on BitTorrent investigations, to include the BitTorrent Overview, ICAC BitTorrent Update and Refresher, Corroborating BitTorrent Investigations, and interview techniques in P2P Investigations. In the course of investigating crimes related to the sexual exploitation of children, I have observed and reviewed numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media, including computer media. I have been involved in numerous online child sexual exploitation investigations and am very familiar with the tactics used by child pornography offenders who collect child pornographic material and those who seek to exploit children.

5. In addition, over the course of this investigation, I have conferred with other investigators who have conducted numerous investigations and executed numerous search and arrest warrants which involved child exploitation and/or child pornography offenses.

STATUTORY AUTHORITY

6. This application is part of an investigation into the alleged knowing distribution and possession of child pornography. 18 U.S.C. § 2252A(a)(2) prohibits a person from knowingly receiving and distributing any child pornography using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing any child pornography that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer.

7. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts set forth in this affidavit are based in part on my personal knowledge, information obtained during my participation in this investigation, information from others, including law enforcement officers, my review of documents and computer records related to this investigation, and information gained through my training and experience.

DEFINITIONS

8. "Child pornography" includes any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. 18 U.S.C. § 2256(8).

9. "Child Erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not, in and of themselves, legally obscene or that do not necessarily depict minors in sexually explicit conduct.

10. "Sexually explicit conduct" means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

11. "Minor" means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

12. "Chat" refers to any kind of communication over the Internet that offers a real-time transmission of text messages from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

13. "Computer," as used herein, is defined pursuant to 18 U.S.C. § 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device." These devices include but are not limited to any data-processing hardware (such as central processing units, memory typewriters, mobile "smart" telephones, tablets, and self-contained "laptop" or "notebook" computers).

14. "Computer hardware," as used herein, consists of all equipment which can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

15. "Computer software," as used herein, is digital information which can be interpreted by a computer and any of its related components to direct the way they work. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.

16. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

17. "Internet Service Providers" ("ISPs"), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment. ISPs can offer a range of options in providing access to the Internet including telephone based dial-up, broadband based access via digital subscriber line ("DSL") or cable television, dedicated circuits, or satellite based subscription. ISPs typically charge a fee based upon the type of connection and volume of data, called bandwidth, which the connection supports. Many ISPs assign each subscriber an account name – a user name or screen name, an "e-mail address," an e-mail mailbox, and a personal password selected by the subscriber. By using a computer equipped with a modem, the subscriber can establish communication with an Internet Service Provider ("ISP") over a telephone line, through a cable system or via satellite, and can access the Internet by using his or her account name and personal password.

18. "Internet Protocol address" or "IP address" refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a

different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the Internet. IP addresses are also used by computer servers, including web servers, to communicate with other computers.

19. The terms "records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks ("DVDs"), Personal Digital Assistants ("PDAs"), Multi Media Cards ("MMCs"), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

BACKGROUND ON PEER TO PEER SOFTWARE

20. Peer-to-peer ("P2P") file-sharing is a method of communication available to Internet users through the use of special software such as BitTorrent. Computers linked together through the Internet using this software form a network that allows for the sharing of digital files between users on the network. These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all of the information is first deposited before it is distributed. A user first obtains

the P2P software, which can be downloaded from the Internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. However, only files that are specifically stored in shared folders are exchanged. Therefore, a user needs simply to move a file from one folder to another to stop the distribution across the Internet. Further, once a file or files are placed in a shared folder its distribution is dependent only on the machine being turned on and connected to the Internet.

21. BitTorrent is one type of P2P file-sharing protocol. Users of the BitTorrent network wishing to share new content will use a BitTorrent client to create a "torrent" file for the file or group of files they wish to share. A torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Torrent files may be referenced by their "infohash", which uniquely identifies the torrent based on the file(s) associated with the torrent file. To download file(s) from other users on the BitTorrent network, a user typically obtains a torrent file. The BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts of the actual file(s) being sought. The download of the content referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software.

22. One of the advantages of P2P file-sharing is that multiple files may be downloaded at the same time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading a movie file may actually receive parts of the movie from multiple computers. The advantage of this is that it

speeds up the time it takes to download the file. It is possible to also download the file or files from only one computer.

23. The BitTorrent Network bases all of its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the digital fingerprinting of data. Once you check a file or files with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file. The SHA1 hash is the current Federal Information Processing and Digital Signature Algorithm. The SHA1 is secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

PROBABLE CAUSE

24. During the month of May 2022, Detective LaRoche and I were monitoring the Nashua Police Department Undercover BitTorrent software and began observing downloads of investigate interest from an IP address geo-locating to the Nashua, NH area. This investigation focused on users sharing child sexual abuse material on the BitTorrent Network. The software used by law enforcement uses SHA1 hash values to identify files being shared on the network that have been previously determined to contain child pornography and / or related material. When the software recognizes the SHA1 hash value of such files on the network, it automatically tries to download them. Further, the BitTorrent software used by law enforcement uses a single-source download protocol. In other words, when the software identifies a BitTorrent user that has suspected files of child pornography available for download, it will initiate a download of the entire file from that single user, as opposed to downloading portions of the target file from multiple users.

25. In total, during the month of May 2022, the target IP address connected with the Undercover BitTorrent software on 12 occasions. On each of these occasions, the UC software recognized and downloaded or attempted to download files of investigative interest containing child sexual abuse material (CSAM) from the target IP address. A selection of the successful downloads is outlined in the following paragraphs.

26. On May 07, 2022, the UC BitTorrent software identified a torrent of investigative interest that was available for download from the IP address 73.114.175.238. The SHA1 infohash associated with the torrent was one that had been previously determined to contain CSAM. The UC BitTorrent software connected with the target IP address and successfully downloaded 3 complete files. One of the downloaded files is described as:

Filename: !!!New!!! (Pthc) Nina 2 (7Yo Bj) AND 7yo_suck_2

Description: two minute and thirteen second video of a prepubescent female and adult male. The female is lying on her back naked on a bed. The video first shows different areas of the female's body then transitions to the adult male inserting his penis into the prepubescent female's mouth. In identifying the female depicted in the video as prepubescent, I am relying on her body size, body structure, facial features, lack of breast development, and lack of pubic hair.

27. On May 08, 2022, the UC BitTorrent software identified a torrent of investigative interest that was available for download from the IP address 73.114.175.238. The SHA1 infohash associated with the torrent was one that had been previously determined to contain CSAM. The UC BitTorrent software connected with the target IP address and successfully downloaded 26 complete files. One of the downloaded files is described as:

Filename: 6Yo Girl Has Sweet Orgasm When Daddy Stimulates Her Pussy With Vibrator, Sound (Pthc Babyj Hussyfan

Description: three minute video involving a prepubescent female. The prepubescent female starts off clothed on a bed and removes her pants while lifting her legs in the air, exposing her vaginal area. An unknown individual is rubbing/inserting a purple object on the prepubescent female's vaginal area as the prepubescent female keeps her legs up in the air and spread. During this time, the camera moves to the prepubescent females face and her vaginal area. As the video continues, the prepubescent female is lying on her back holding the purple object in her hand rubbing/inserting it on her vaginal area. At the end of the video, the prepubescent female is on her hands/knees and the unknown individual is rubbing/inserting the purple object near the prepubescent female's anal opening. In identifying the female depicted in the video as prepubescent, I rely on her body size, body structure, facial features, and lack of pubic hair.

28. On May 11, 2022, the UC BitTorrent software identified a torrent of investigative interest that was available for download from the IP address 73.114.175.238. The SHA1 infohash associated with the torrent was one that had been previously determined to contain CSAM. The UC BitTorrent software connected with the target IP address and successfully downloaded 47 complete files. One of the downloaded files is described as:

Filename: PTHC.2013.NEW.0602.Awesome.3yo.Girl.Suck.Dad.Great.Blowjob

Description: fifteen second video of an adult male inserting his penis into the mouth of a prepubescent female. In identifying the female depicted in the video as prepubescent, I base this conclusion off her body size, body structure, facial features, and lack of breast development.

29. On May 28, 2022, the UC BitTorrent software identified a torrent of investigative interest that was available for download from the IP address 73.114.175.238. The SHA1 infohash associated with the torrent was one that had been previously determined to contain

CSAM. The UC BitTorrent software connected with the target IP address and successfully downloaded 18 complete files. One of the downloaded files is described as:

Filename: Andina 5Yo Incest Slut Child Anal And Face Cum

Description: Eleven minute and six second video of a prepubescent female lying on her back on a bed with her dress pulled up exposing a portion of her upper body and lower body. A male inserts his finger into the prepubescent female's vaginal opening then begins to have sexual intercourse with the prepubescent female in various positions. As the video continues, the male begins to rub his penis on the prepubescent female's face and insert it into her mouth, eventually ejaculating in the area of her mouth. In identifying the female depicted in the video as prepubescent, I rely on her body size, body structure, facial features, lack of breast development, and lack of pubic hair.

30. Upon reviewing each connection, I observed the status was listed as "terminated". This regularly occurs during undercover BitTorrent investigations as the software is primarily designed for users to receive and share files, which the law enforcement software does not do. The software used by law enforcement only receives files of investigative interest thus the sessions regularly terminate without completing the full download of all of the files within a particular torrent.

31. I completed a summons for the IP address 73.114.175.238 and various port numbers on the dates/times in which connections occurred. I later received the results of the summons from Comcast, which showed the subscriber for each instance was the Crane Restaurant, located at 113 W Pearl Street, Unit 2, Nashua, NH.

32. On May 31, 2022, I conducted a scan for wireless internet signals while outside of Crane Restaurant. Crane Restaurant is a single story building with an alley way on its left side

and the business Waypoint located on its right side. During this time, I observed a wireless signal titled “CraneRestaurant” which was locked. Through my training and experience, I know a “locked” signal will require a password to access.

33. On June 01, 2022, at approximately 12:20 P.M., Detective McDermott and Detective Murray, working in an undercover capacity, went into Crane Restaurant and had lunch. While inside, the wireless internet password did not appear posted anywhere; however it was discovered that a wireless internet signal was available. Detective McDermott requested the password for the wireless internet from the hostess, and she provided the password "sushidave". Detective McDermott was able to log on to the wireless internet “CraneRestaurant” successfully using this password. Using a publicly-available online database, Detective McDermott identified the IP address for Crane Restaurant as 73.114.175.238. This matched the IP address from the BitTorrent downloads as well as the subscriber information provided by Comcast in response to the HSI summons. Within the restaurant during this time period, detectives observed a female hostess as well as two male workers who were working in the kitchen. There was also a female child who was seated by the kitchen area and appeared to be associated with the employees.

34. Continuing on June 01, 2022, at approximately 5:30 P.M., Detective LaRoche and I responded to Crane Restaurant. Using the ruse of investigating a suspicious death reported nearby the previous day, we spoke with employees Eric Oou, Selena Li, and Dwayne Frechette. There was one additional employee in the kitchen who Li did not wish to identify. Li advised that these four individuals were the only employees of the restaurant. Li also informed us that the restaurant is open from 12 P.M. to 9 P.M. everyday but Tuesday. Although the hours are 12 P.M. to 9 P.M., Li, Oou, and Frechette advised that they regularly remain at the restaurant after 9 P.M.

This is of investigative interest as the downloads from BitTorrent have not occurred on Tuesdays and primarily have occurred when the restaurant is open, or just after its closing time.

35. When we entered the restaurant, we observed Frechette seated at the bar in the far right corner on his laptop computer. As we were speaking with Oou and Li, Frechette shut his laptop and came over to introduce himself, questioning what we were there to investigate. Frechette advised he helps with take-out orders for the restaurant, and spends most of his time at the restaurant when he is not working. In regards to the past three days, he advised he was at the restaurant on Saturday, Sunday and Monday. This is of investigative interest as a download occurred on Sunday May 29, 2022 at 9:07 P.M., which is after the restaurant had closed. According to Frechette, he would have had access to the restaurant after closing.

36. Beginning in late May and continuing through June 2022, I began surveillance on the Crane Restaurant and observed Frechette was regularly at the restaurant during and after business hours. Furthermore, as stated by Frechette, the surveillance showed he was delivering food for the restaurant as he would routinely exit the restaurant through the front or rear door carrying bags which were consistent with food packaging, enter his vehicle, go directly to an address, then back to the restaurant. Additionally, after Frechette left the restaurant once it was closed he routinely traveled to a nearby parking garage where he stayed overnight. Based on this information, it appeared as though Frechette was living out of his vehicle.

37. On July 08, 2022 I completed a search warrant package for the Crane Restaurant and any employees or subcontractors, such as delivery drivers within. Among other things, the search warrant authorized the search and seizure of electronics found within the restaurant and on the person of employees or subcontractors, such as delivery drivers within. The search

warrant package was reviewed and signed into effect by United States Magistrate Judge Andrea Johnstone.

38. On July 11, 2022, members of HSI and the Nashua Police Department executed the aforementioned search warrant. During the execution, SA Mike Perrella and I conducted a voluntary interview[1] with FRECHETTE. FRECHETTE made admissions to having the BitTorrent software on his cell phone, later determined to be a device located within the restaurant. A preliminary search of this device showed the phone was linked to FRECHETTE's computer by way of Google accounts. FRECHETTE informed SA Perrella and I, he has purchased multiple cell phones and stated one of them was currently in his vehicle. For this specific phone, FRECHETTE stated it did not have cell phone service, and could only be used by connecting to a wireless internet. This phone was later found to be the SUBJECT DEVICE. After approximately one hour, FRECHETTE advised he wished to consult with an attorney before continuing to speak with us.

39. Given FRECHETTE's statements about additional electronics within his vehicle, the vehicle was secured at the Nashua Police Department pending a search warrant.

40. A search of the phone within the restaurant confirmed the BitTorrent software was present and also showed 290 images of child sexual abuse material. A description of one CSAM files is:

> A digital image of a prepubescent female lying on her side visible from the chest up to her face. The female has no shirt on. A male is inserting his genitalia into the females

[1] Frechette was read his Miranda Rights and agreed to speak with investigators without an attorney present. The interview and audio and video recorded.

mouth. In identifying the female depicted in the image as prepubescent, I base this conclusion off her facial features, body size, and lack of breast development

41. Interviews were conducted with three additional employees of the restaurant, Lian Yongbing, Yongxiu Ou, and Duanyu Li who advised they had no knowledge of BitTorrent. Searches of their phones showed BitTorrent was not downloaded nor was CSAM present.

42. On July 12, 2022, a search warrant was issued by United States Magistrate Judge Andrea Johnstone for FRECHETTE's vehicle (22-mj-144-01-AJ). During a search of the vehicle, the SUBJECT DEVICE was located within.

43. On July 14, 2022, I completed a partial extraction of the SUBJECT DEVICE but due to the fact it was locked and the password was unknown, only a partial extraction was completed. A review of this extraction did not provide any items of investigative interest.

44. On July 26, 2023, FRECHETTE was arrested after being indicted in the United States District Court for the District of New Hampshire for violations of Title 18, United States Code, Section 2252A(a)(5)(B), which relates to the possession and access with intent to view child pornography. FRECHETTE's case is still pending before this court.

45. The SUBJECT DEVICE has remained at all times in the custody and control of HSI since the initial extraction was performed. Due to the security of the device and its operating system in 2022, the initial forensic examination was unsuccessful in extracting all the potentially relevant data from the device. Since this initial attempt, there have been several updates and improvements to the hardware and software used by HSI to conduct extractions of mobile devices. These updates may provide an ability to complete a full extraction on the device which may provide further evidence which was not available in 2022.

CONCLUSION

46. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of the crimes of distribution and possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5)(B) may be located within the SUBJECT DEVICE. I therefore seek a warrant to search the SUBJECT DEVICE, as further described in Attachment A, and to seize and search the items described in Attachment B.

47. I am aware that the recovery of data by a computer forensic analyst takes significant time; much the way recovery of narcotics must later be forensically evaluated in a lab, digital evidence will also undergo a similar process. For this reason, the "return" inventory will contain a list of only the tangible items recovered from the premises. Unless otherwise ordered by the Court, the return will not include evidence later identified by a computer forensic examiner.

/s/ Adam Rayho
Adam Rayho
Special Agent
Homeland Security Investigations

Sworn and subscribed before me this 30th day of April 2024.

Honorable Talesha Saint-Marc
United States Magistrate Judge
District of New Hampshire

ATTACHMENT A

PROPERTY TO BE SEARCHED

The digital device identified below, seized pursuant to 22-mj-144-01-AJ and presently in the custody of HSI Manchester, 275 Chestnut Street, Manchester, New Hampshire:

One Samsung Galaxy A03, IMEI 357815981123565

ATTACHMENT B

ITEMS TO BE SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2252A(a)(5)(B) and 2252A(a)(2):

1. All records relating to violations of 18 U.S.C. §§ 2252A(a)(5)(B), 2252A(a)(2) in any form they may be found, including:

a. records and visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256;

b. records or information pertaining to an interest in child pornography;

c. records or information pertaining to the possession, receipt, transportation, or distribution of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

d. records or information of and relating to visual depictions that have been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct as defined in 18 U.S.C. § 2256, including the record or information used to create the visual depiction;

e. records or information pertaining to BitTorrent;

f. photo-editing software and records or information relating to photo-editing software;

2. With regard to the SUBJECT DEVICE:

a. evidence of who used, owned, or controlled the SUBJECT DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the SUBJECT DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the SUBJECT DEVICE of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICE;

f. evidence of the times the SUBJECT DEVICE was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICE;

h. documentation and manuals that may be necessary to access the SUBJECT DEVICE or to conduct a forensic examination of the SUBJECT DEVICE;

i. contextual information necessary to understand the evidence described in this attachment.